Notice of Allowability	**Application No.** 09/451,090	**Applicant(s)** SANDHU ET AL.	
	Examiner Khanh Dinh	**Art Unit** 2151	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *6/29/2005*.

2. ☒ The allowed claim(s) is/are *79,80,83-90,92-95 and 97-121*.

3. ☐ The drawings filed on _____ are accepted by the Examiner.

4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
   1. ☐ Certified copies of the priority documents have been received.
   2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
   3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

6. ☒ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☒ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
   1) ☒ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

7. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☒ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☒ Examiner's Amendment/Comment
8. ☐ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

EXAMINER'S AMENDMENT

1. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with David Grossman (Reg. No.42,609) on 6/29/2005.

The application has been amended as follows:

IN THE CLAIMS:

Please **cancel** claim 82.

Please **amend** claims as follows:

Claim 79 (Currently Amended): A system for transferring [[of]] secure data on a network comprising:

a) a client capable of presenting conforming client data;

b) a server capable of using said conforming client data to create at least two secure cookies, each of said at least two secure cookies including:

i) a domain field capable of holding domain data to associate said secure cookie to a domain where said secure cookie is valid;

ii) at least one name field capable of holding name data;

iii) at least one value field capable of holding value data derived from said conforming client data; and

iv) an expiration field capable of holding cookie expiration data;

c) a network capable of transporting at least one of said at least two secure cookies between said server and said client;

d) a client storage means capable of storing at least one of said at least two secure cookies; and

e) a secure attribute service between said client and said server using said at least one of said at least two secure cookies,

wherein:

i) at least one of said at least two secure cookies is a key cookie containing an encrypted session key, said session key capable of encrypting said value data contained in another of said at least two secure cookies; and

ii) said secure attribute service includes said server being configured to authenticate said client by comparing said conforming client data with said value data.

Claim 80 (previously presented): A system according to claim 79, wherein said client is a web browser.

Claim 81 (canceled)

Claim 82 (canceled): ~~A system according to claim 79, wherein said secure attribute service includes said server authenticating said client by comparing said conforming client data with said value data.~~

Claim 83 (previously presented): A system according to claim 119, wherein said authentication cookie is an IP cookie and said conforming client data includes the IP address of said client.

Claim 84 (previously presented): A system according to claim 119, wherein said authentication cookie is a password cookie and said conforming client data includes a password.

Claim 85 (previously presented): A system according to claim 84, wherein said password is processed using a hashing algorithm.

Claim 86 (previously presented): A system according to claim 84, wherein said password is processed using an encryption algorithm.

Claim 87 (previously presented): A system according to claim 119, wherein said authentication cookie is a sign cookie and said conforming client data includes a digital signature on a timestamp.

Claim 88 (previously presented): A system according to claim 119, further including a secret-key based authentication service.

Claim 89 (previously presented): A system according to claim 88, and wherein said authentication cookie is a KT cookie and said conforming client data includes a Kerberos ticket created using a Kerberos protocol.

Claim 90 (previously presented): A system according to claim 79, wherein at least one of said at least two secure cookies includes a multitude of secure cookies.

Claim 91 (canceled)

Claim 92 (previously presented): A system according to claim 118, wherein said seal cookie includes an integrity check value.

Claim 93 (previously presented): A system according to claim 118, wherein said seal cookie includes the signature of a message digest signed using a private key.

Claim 94 (previously presented): A system according to claim 79, wherein at least one of said at least one name field and at least one of said at least one value field are a pair.

Claim 95 (previously presented): A system according to claim 79, wherein at least one of said at least two secure cookies further includes a flag, said flag specifying whether all machines within said domain referenced by said domain data can access said value data.

Claim 96 (canceled)

Claim 97 (previously presented): A system according to claim 79, wherein at least one of said at least two secure cookies is used in an electronic transaction.

Claim 98 (previously presented): A system according to claim 79, wherein said system is part of a role based access control system and at least one of said at least two secure cookies is used in assigning client roles.

Claim 99 (Currently Amended): A method for [[the]] transferring [[of]] secure data on a network including the steps of:

a) a client making a request from a server;

b) said server retrieving conforming client data;

c) said server creating at least two secure cookies, each of said at least two secure cookies including selected conforming client data, said selected conforming data including at least some of said conforming client data;

d) said server transmitting at least one of said at least two secure cookies to said client;

e) said client storing at least one of said at least two secure cookies;

f) said client presenting to a related server at least one of said stored at least two secure cookies with a second request, said related server residing on the same domain as said server;

g) said related server making a determination of whether at least one of said at least one retrieved stored at least two secure cookies contains said selected conforming client data; and

h) said related server fulfilling said second request if said determination is positive;

wherein at least one of said at least two secure cookies is a key cookie containing an encrypted session key, said session key capable of encrypting said value data contained in another of said at least two secure cookies.

Claim 100 (previously presented): A method of claim 99 wherein at least some of said conforming client data is retrieved from said client.

Claim 101 (previously presented): A method of claim 99, wherein said conforming client data includes a client's IP address.

Claim 102 (previously presented): A method of claim 99, wherein said conforming client data includes a password.

Claim 103 (previously presented): A method of claim 99, wherein said conforming client data includes a Kerberos ticket.

Claim 104 (previously presented): A method of claim 99, wherein said conforming client data includes a digital signature.

Claim 105 (previously presented): A method of claim 104, wherein said determination further includes verifying that said digital signature belongs to said client.

Claim 106 (previously presented): A method of claim 99, further including the step of said server encrypting at least some of said selected conforming client data.

Claim 107 (previously presented): A method of claim 106, wherein said encrypting uses a public key.

Claim 108 (previously presented): A method of claim 106, wherein said encrypting uses a secret key.

Claim 109 (previously presented): A method of claim 106, further including the step of said server decrypting said encrypted selected conforming client data using a private key.

Claim 110 (previously presented): A method of claim 106, further including the step of said server decrypting said encrypted selected conforming client data using a secret key.

Claim 111 (previously presented): A method of claim 99, further including the step of said server hashing at least some of said conforming client data.

Claim 112 (previously presented): A method of claim 99, wherein said conforming client data includes data derived from at least one item from the group consisting of:

a) the client's IP address;

b) a password;

c) a Kerberos ticket;

d) credit card data;

e) social security number;

f) a digital signature of the client; and

g) a home address.

Claim 113 (previously presented): A method of claim 99, wherein said determination is positive only if said selected conforming client data was retrieved by said server from said client during the current session.

Claim 114 (previously presented): A method of claim 99, wherein said secure cookie contains a digital signature of said client on a time-stamp.

Claim 115 (previously presented): A method of claim 99, further including the step of providing integrity to at least one of said at least two secure cookies comprising:

a) said server creating integrity data from at least one of said at least two secure cookies, said integrity data including at least one item selected from the group:

i) encrypted said selected conforming client data;

ii) a digital signature; and

iii) a message digest;

b) said server inputting said integrity data into a seal cookie; and

c) said server storing said seal cookie.

Claim 116 (previously presented): A method of claim 99, wherein said request is part of an electronic transaction.

Claim 117 (previously presented): A method of claim 99, wherein said request is part of an attribute-based access control function.

Claim 118 (Currently Amended): A system for transferring [[of]] secure data on a network comprising:

a) a client capable of presenting conforming client data;

b) a server capable of using said conforming client data to create at least two secure cookies, each of said at least two secure cookies including:

i) a domain field capable of holding domain data to associate said secure cookie to a domain where said secure cookie is valid;

ii) at least one name field capable of holding name data;

iii) at least one value field capable of holding value data derived from said conforming client data; and

iv) an expiration field capable of holding cookie expiration data;

c) a network capable of transporting at least one of said at least two secure cookies between said server and said client;

d) a client storage means capable of storing at least one of said at least two secure cookies; and

e) a secure attribute service between said client and said server using said at least one of said at least two secure cookies, said secure attribute service includes said server being configured to authenticate said client by comparing said conforming client data with said value data; and

wherein at least one of said at least two secure cookies is one of the following:

i) a seal cookie, capable of being used by said server to determine if at least one of another of said at least two secure cookies has been altered; and

ii) a key cookie containing an encrypted session key, said session key capable of encrypting said value data contained in another of said at least two secure cookies.

Claim 119 (previously presented): A system according to claim 79, wherein at least one of said at least two secure cookies is an authentication cookie.

Claim 120 (Currently Amended): A method for [[the]] transferring [[of]] secure data on a network including the steps of:

a) a client making a request from a server;

b) said server retrieving conforming client data;

c) said server creating at least two secure cookies, each of said at least two secure cookies including selected conforming client data, said selected conforming data including at least some of said conforming client data;

d) said server transmitting at least one of said at least two secure cookies to said client;

e) said client storing at least one of said at least two secure cookies;

f) said client presenting to a related server at least one of said stored at least two secure cookies with a second request, said related server residing on the same domain as said server;

g) said related server making a determination of whether at least one of said at least one retrieved stored at least two secure cookies contains said selected conforming client data; and

h) said related server fulfilling said second request if said determination is positive;

wherein at least one of said at least two secure cookies is one of the following:

i) a seal cookie, capable of being used by said server to determine if at least one of another of said at least two secure cookies has been altered; and

ii) a key cookie containing an encrypted session key, said session key capable of encrypting said value data contained in another of said at least two secure cookies.

Claim 121 (previously presented): A method according to claim 99, wherein at least one of said at least two secure cookies is an authentication cookie.

Allowable Subject Matter

2. Claims 79, 80, 83-90, 92-95 and 97-121 are allowed.

3. The following is an examiner's statement of reasons for allowance:

The above mention claims are allowable over the prior art of record does not appear to each or render obvious the claimed limitations in combination with the specific added limitations as recited in independent claims and subsequent dependent claims.

For independent claims 79 and 99, none of the cited prior art discloses or teaches a method for transferring

secure data on a network comprising a combination of: said server creating at least two secure cookies, each of said at least two secure cookies including selected conforming client data, said selected conforming data including at least some of said conforming client data wherein at least one of said at least two secure cookies is a key cookie containing an encrypted session key, said session key capable of encrypting said value data contained in another of said at least two secure cookies.

For independent claims 118 and 120, none of the cited prior art discloses or teaches a method for transferring secure data on a network comprising a combination of: said server creating at least two secure cookies, each of said at least two secure cookies including selected conforming client data, said selected conforming data including at least some of said conforming client data wherein at least one of said at least two secure cookies is a key cookie containing an encrypted session key, said session key capable of encrypting said value data contained in another of said at least two secure cookies including a seal cookie, capable of being used by said server to determine if at least one of another of said at least two secure cookies has been altered.

Conclusion

4. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Khanh Dinh whose telephone number is (571) 272-3936. The examiner can normally be reached on Monday through Friday from 8:00 A.m. to 5:00 P.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Zarni Maung, can be reached on (571) 272-3939. The fax phone number for this group is (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Khanh Dinh

Khanh Dinh
Patent Examiner
Art Unit 2151
6/30/2005